IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

VANDERBILT UNIVERSITY, *Plaintiff*, v. SCHOLASTIC, INC.; HOUGHTON MIFFLIN HARCOURT PUBLISHING COMPANY; and TED S. HASSELBRING, *Defendants*.	Civil Action No. 3:18-CV-00046 Chief Judge Waverly D. Crenshaw, Jr. Magistrate Judge Jeffery S. Frensley JURY DEMAND
SCHOLASTIC, INC., *Counterclaim-Plaintiff*, v. VANDERBILT UNIVERSITY, *Counterclaim-Defendant*.	
TED S. HASSELBRING, *Counterclaim-Plaintiff*, v. VANDERBILT UNIVERSITY, *Counterclaim-Defendant*.	

DEFENDANT HASSELBRING'S RESPONSE IN OPPOSITION
TO VANDERBILT'S MOTION FOR PROTECTIVE ORDER

Vanderbilt has taken advantage of unforeseeable circumstances and intrusive technology to obtain and review Defendant Hasselbring's confidential communications, all of which originated from his privately-owned devices (a laptop computer and his cell phone), using a Gmail account created and utilized for the express purpose of avoiding any risk that those

communications could be intercepted by Vanderbilt. It now seeks to review and disclose additional attorney-client privileged communications between Defendant and his legal counsel in this lawsuit. Just as disturbingly, Vanderbilt came into possession of this material—material that it knew or should have known was confidential, and in many cases, privileged—no later than June 2, 2019, but failed to notify Hasselbring or his counsel for over three months.[1] At least for that interim period, Vanderbilt maintained the ability to monitor privileged communications about this case while counsel continued to communicate with Hasselbring via his Gmail account that was utilized for the specific purpose of maintaining confidentiality, not aware of Vanderbilt's ability to capture those communications.

Vanderbilt's excuse for this conduct is that Hasselbring gave up all expectation of privacy because on a number of occasions before and after the commencement of this litigation he utilized the Vanderbilt Virtual Private Network ("VPN") on computers that had been purchased for Hasselbring's use and necessarily saw a legend that warned that users of the VPN have "no explicit or implicit expectation of privacy" while using the VPN. As the discussion below demonstrates, Hasselbring's occasional use of the Vanderbilt VPN (for reasons unrelated to this litigation) has nothing to do with this case, because it is not the mechanism by which Vanderbilt intercepted his communications with counsel.

This is not the typical employee email case, in which an employee communicates with his or her attorneys using a computer, email account, and/or internet services unambiguously provided by an employer. In this case, Hasselbring's email communications with counsel occurred exclusively by means of a private, web-based, password-protected, Gmail account used on several

[1] Vanderbilt offers no explanation for the three-month delay in informing Hasselbring's counsel that it had come into possession of confidential and privileged material or that it could "see" emails being sent between Hasselbring and his legal counsel.

privately purchased and owned devices connected to private, non-Vanderbilt internet sources. Apparently, these precautions were thwarted by unforeseeable circumstances, the most significant of which was Vanderbilt's use of a computer program known as "CrashPlan." Whatever warnings or explanation might have been offered by Vanderbilt regarding CrashPlan (we are aware of none), it is inconceivable that Vanderbilt warned Hasselbring that CrashPlan could access and capture emails sent from a non-Vanderbilt computer, utilizing a non-Vanderbilt email account, as was the case here.

ADDITIONAL FACTUAL BACKGROUND

Vanderbilt claims to possess a total of 73 emails between Hasselbring and his counsel in this case. [Dkt. 163-3 at ¶ 13.] While Vanderbilt has consistently refused to identify or give Hasselbring access to these emails, Vanderbilt itself has admitted that at least 29 of those emails would otherwise be privileged. It may well be that the remaining 44, which Vanderbilt claims to be devoid of legal advice or factual discussion, are privileged as well. In any case, Vanderbilt admits that they are communications with counsel.[2]

Hasselbring took precautions to protect his communications with counsel in this case—precautions that anyone would consider more than adequate. Chief among them was the creation and use of a private, web-based, password-protected email address provided by Gmail.com. [*See* Exhibit A, Declaration of Ted. S. Hasselbring ("Hasselbring Decl.") at ¶¶ 4-5.] Since its creation,

[2] In addition to the privileged emails, Vanderbilt has already produced four different versions of a draft memorandum Hasselbring prepared at direction and for the benefit of counsel regarding certain factual issues raised by Vanderbilt's Complaint. Hasselbring informed all counsel of the privileged nature of these documents immediately upon discovery and Vanderbilt agreed to screen them as they have screened the privileged emails at issue in this Motion. Until Hasselbring is permitted to take discovery, it is impossible to know how these documents came to be captured by Vanderbilt's systems. Hasselbring reserves all rights on that issue. Hasselbring similarly reserves his right as to the other, vaguely defined "potentially privileged" emails described in Vanderbilt's Motion, about which he can make no argument without further discovery.

this Gmail account has been the exclusive means by which Hasselbring and his counsel have communicated by email. [Hasselbring Decl. at ¶ 6.] To the best of Hasselbring's recollection, these email communications have all been sent exclusively from personal electronic devices he purchased himself, none of which have ever been provided to Vanderbilt for any reason. [Hasselbring Decl. at ¶ 7.] This was done with the expectation that all emails sent and received on this Gmail account would be private, and as an explicit alternative to communications using Hasselbring's Vanderbilt-provided email address. [Hasselbring Decl. at ¶¶ 5-6.]

This means that the otherwise privileged emails at issue could only have been come from Hasselbring's Gmail account, and from Vanderbilt gaining access to that account. The explanation of how this might have occurred demonstrates that the policies on which Vanderbilt relies did not negate Hasselbring's reasonable expectation that his communications with counsel in this case would remain private.[3]

A. Hasselbring's use of a private email account in no way associated with the Vanderbilt "system" was a reasonable and more than sufficient precaution to insure the confidentiality of his communications with counsel.

Vanderbilt's arguments that its "Notice to Users" (displayed when a user connects to the Vanderbilt VPN) or its Acceptable Use Policy (applicable by its terms only to the use of Vanderbilt's "secure network-computing infrastructure") dispel any expectation of privacy Hasselbring would have otherwise possessed are irrelevant: neither his occasional connection to the VPN or use of the Vanderbilt network have anything to do with the way Vanderbilt came to possess Hasselbring's communications with his legal counsel. This is so because he did not utilize the VPN or the devices identified by Mr. Sidiqyar to communicate with his legal counsel—he used

[3] We say "might" because Vanderbilt has refused to permit any discovery pointed at uncovering the who, what, why and when of the CrashPlan application and has filed a second Motion for Protective Order to prevent such discovery. [Dkt. 164; 165.]

his cell phone, laptop computer, and tablet computer (all purchased with his own funds), none of which were used to connect to the Vanderbilt "system." [Hasselbring Decl. at ¶ 7.]

Instead, here is what allowed Vanderbilt to gain access to Hasselbring's Gmail communications with his counsel despite the care taken to safeguards these emails. Unknown to Hasselbring, and without any act of his own, a local copy of his Gmail communications with counsel was apparently created on the computers identified by Mr. Sidiqyar, and these Gmail communications were transmitted to Vanderbilt. While the program is barely mentioned in Vanderbilt's brief, it is apparent that this transmission could only have happened by operation of CrashPlan. A closer examination of this program and how it was installed is crucial.

First, one should keep in mind that Mr. Sidiqyar's discussion of the warnings provided to users of the Vanderbilt system does not claim that Hasselbring received any warning or instruction about the installation or capabilities of CrashPlan, nor has Vanderbilt claimed that such a warning or instruction was provided. [*See generally* Dkt. 163-1.] Hasselbring does not recall receiving any explanation of Vanderbilt's ability to access and review CrashPlan-created files, nor does Vanderbilt claim that such an explanation was provided. [Hasselbring Decl. at ¶ 24.] In any case, he acted reasonably in not considering the possibility that Vanderbilt could use CrashPlan (or any other program) to obtain copies of emails sent or received in his Gmail account and utilizing his other devices that had not been furnished or maintained by Vanderbilt or its IT department. Hasselbring reasonably (but incorrectly, as it turns out) believed Vanderbilt could only access and view the contents of, at most, some portion of the content of the computers identified by Mr. Sidiqyar if physical or remote access to those computers was provided directly to Vanderbilt's IT department, which has not occurred since this lawsuit has been pending. [Hasselbring Decl. at ¶ 14.] It is worth reiterating that, regardless of his understanding of Vanderbilt's ability to access the

contents of these computers, Hasselbring did not expect that those contents would include copies of his email communications with counsel sent by means of his Gmail account on other, privately-purchased devices while not connected to Vanderbilt's internet or other systems. [Hasselbring Decl. at ¶ 5.]

So how did CrashPlan, a program installed on the computers identified by Mr. Sidiqyar, gain access to Gmail communications that originated on Hasselbring's privately-purchased devices? Vanderbilt's apparent possession of such communications compels the conclusion that Hasselbring must have *accessed* his Gmail account from one or both those computers, a possibility which he acknowledges. [Hasselbring Decl. at ¶ 9.] But Hasselbring was not aware that the mere act of accessing his Gmail account (not even sending a message using Gmail—just opening the Gmail account) on these computers would create a copy of *all* communications contained in his Gmail account on the computers identified by Mr. Sidiqyar. [Hasselbring Decl. at ¶¶ 5, 14, 24.] Nor was he aware that, if such a copy was created, it would be accessible by Vanderbilt by virtue of CrashPlan. [*Id.*]

B. Vanderbilt allowed Hasselbring to keep and use the computers described in Mr. Sidiqyar's Declaration without any limitations or warnings.

Without regard to the critical, dispositive fact that Hasselbring communicated with his counsel exclusively using his privately-owned devices, Vanderbilt claims that the communications at issue were "created and used by Hasselbring while on Vanderbilt's systems." Vanderbilt is incorrect. Even if he had utilized the computers identified by Mr. Sidiqyar to communicate with counsel (he did not) via his Gmail account (the exclusive means utilized to communicate with counsel about this case), Hasselbring did not consider that those computers remained part of Vanderbilt's system (however the term "Vanderbilt's system" is defined), and was unaware that those computers could be remotely monitored. [Hasselbring Decl. at ¶¶ 13-14.]

But consider the implications of Vanderbilt's position even if the privileged communications were created and sent on the Gmail account while on the computers identified by Mr. Sidiqyar—computers that had been in Hasselbring's exclusive possession for years. While Hasselbring was employed as a Vanderbilt professor, funds from the Read 180 license (which would not have existed but for Hasselbring's talents and efforts) were used to purchase a MacBook Pro laptop and iMac desktop computer for Hasselbring's use. [Hasselbring Decl. at ¶ 8.] These computers are identified by serial number in Mr. Sidiqyar's Declaration. [*Id.*] Hasselbring does not recall being asked to sign any documentation regarding the ownership, control, or acceptable uses of those computers when they were provided to him, and Vanderbilt has produced no evidence that he signed such documentation. [Hasselbring Decl. at ¶ 10.]

In 2017, Hasselbring retired and, while cleaning out his office, took both computers with him. [Hasselbring Decl. at ¶ 11.] Vanderbilt did not object. [*Id.*] To the best of Hasselbring's recollection, Vanderbilt also did not warn him that these computers remained Vanderbilt property notwithstanding his retirement and removal of them from Vanderbilt's campus, that there were any limitations on their use after his retirement, or, most critically, that Vanderbilt could remotely access data stored on those computers. [Hasselbring Decl. at ¶ 12.] Vanderbilt has not produced evidence that they provided such a warning. Hasselbring accordingly treated them as his personal property and was unaware that Vanderbilt retained any right in them or access to them. [Hasselbring Decl. at ¶ 13.] He certainly did not take any steps that he understood as creating the potential for Vanderbilt to access the contents of those computers, such as taking them on campus, connecting them to Vanderbilt's Wi-Fi, or providing access to Vanderbilt's IT department. [Hasselbring Decl. at ¶ 14.]

C. Vanderbilt seized the emails at issue through the operation of "CrashPlan."

Unfortunately, it is now clear that Hasselbring's understanding was incorrect. As set forth in Mr. Sidiqyar's Declaration, the CrashPlan application was installed on these computers. [Dkt. 163-1 at ¶ 21.] According to Mr. Sidiqyar, that program allowed Vanderbilt to copy and retrieve "the native documents on a user's machine"—including, apparently, back-up files of web-based emails sent on a private email server, using private devices, over private internet connections—"without physical access to the Vanderbilt-issued computer." [Dkt. 163-1 at ¶ 22.]

The mechanism by which this copying occurred bears emphasis. According to Mr. Sidiqyar, CrashPlan makes a remote copy of the documents on a given computer "[a]fter a user connects to the internet." [Dkt. 163-1 at ¶ 24.] In other words, all it takes for CrashPlan to operate is an internet connection. (Crucially, connection to the Vanderbilt VPN is irrelevant to the process.) It does not appear that this back-up is preceded by a prompt or warning that it is about to occur, or that it requires any connection to Vanderbilt's internet or other systems. This means that a back-up of some or all "native documents" on a given computer may be copied to the Vanderbilt-accessible cloud when, for example, someone logs onto a computer for the sole purpose of checking the weather or the latest football score, even if not on Vanderbilt's campus or otherwise connected to Vanderbilt's VPN, internet, or other system.

While Vanderbilt has so far declined to permit Hasselbring to take discovery on this issue, Mr. Sidiqyar's Declaration clarifies that the communications at issue came to be in Vanderbilt's possession by means of CrashPlan only, unrelated to any voluntary surrender of these computers to Vanderbilt or (as explained more fully below) any use of Vanderbilt's VPN network or other systems. [*See also* Mills Decl., Dkt. 163-2, at ¶ 8 (explaining that the documents at issue were obtained solely from CrashPlan).]

D. Vanderbilt's Acceptable Use Policy is contradictory and vague.

While we contend that the Acceptable Use Policy has no bearing on the instant dispute (since the emails in question were created and sent using Hasselbring's privately owned devices while not on any Vanderbilt "system"), that policy still warrants scrutiny, since it is the only Vanderbilt policy that could conceivably be relevant to the installation and operation of CrashPlan on the computers identified by Mr. Sidiqyar. As noted above, Hasselbring did not use any Vanderbilt-issued computers, his Vanderbilt email address, or any other Vanderbilt system to send or receive the emails at issue. As such, his actions were not even governed by the policy. And, as also discussed above, Vanderbilt's actions (and inactions) with respect to the computers identified by Mr. Sidiqyar creates significant doubt whether this policy even applied to those computers at all relevant times (*i.e.*, after Hasselbring's retirement), meaning it is unclear whether this Policy would be relevant even if Hasselbring intentionally stored his web-based emails on these computers (which, to be clear, he absolutely did not).

Assuming *arguendo* that the Acceptable Use Policy is applicable on these facts, though, it is far more ambiguous than Vanderbilt's description makes it out to be.[4] With respect to privacy expectations, Vanderbilt relies exclusively upon three sentences contained in Section F of the Policy. These sentences describe two circumstances in which Vanderbilt may "obtain and review any records" (an undefined term) and conclude with the statement users "should not expect that records created, stored, or communicated" on Vanderbilt's systems "will *necessarily* be private."

[4] The Acceptable Use Policy is attached to Mr. Sidiqyar's Declaration as Exhibit 1. [Dkt. 163-1 at 8-11.]

As suggested by the term "necessarily," though, this policy falls far short of the explicit "no expectation of privacy" language contained in (for example) the policies at issue in the cases cited by Vanderbilt. Among other things, the Acceptable Use Policy also provides:

- "Vanderbilt is committed to *protecting the privacy of faculty*, students, staff, patients, and other users of its IT resources, and their electronic communications."
- "The *privacy of all users* and the integrity and operational security of Vanderbilt's information technology system must be *respected by all*."
- "Vanderbilt's IT resources must not be used by anyone to gain or attempt to gain unauthorized access to private information, *even if that information is not securely protected or is otherwise available."*
- "The fact that an individual account and its data may be unprotected does not confer either an ethical or *legal* right to access it."
- "Unauthorized access to private information constitutes a violation of this policy."
- Vanderbilt's "IT professionals" must "[p]reserv[e] confidentiality."

[Dkt. 163-1 at 9-10 (emphasis added).] The only uses explicitly forbidden by the Policy are those which violate the law, Vanderbilt's institutional policies, or its student honor or conduct codes. The Policy even explicitly contemplates that users may store "sensitive personal information" on Vanderbilt's systems, and states that users have the responsibility of "[t]aking care to minimize risks of" disclosure of such information. [Dkt. 163-1, Ex. 1 at § C.1.] The Policy never forbids or even discourages personal use of Vanderbilt's systems; it certainly does not explain that employees may not use Vanderbilt's systems to view communication with their legal counsel.

E. Hasselbring's use of Vanderbilt's VPN is unrelated to Vanderbilt's seizure of his privileged communications, and the "Notice to Users" does not apply.

Perhaps in light of the inherent ambiguities of its Acceptable Use Policy, Vanderbilt instead relies chiefly upon the (relatively) more explicit warnings contained in the "Notice to Users" displayed before accessing Vanderbilt's VPN system (attached as Exhibit 2 to Mr. Sidiqyar's

Declaration, Dkt. 163-1 at 12-13). This Notice to Users has no bearing on this case and is instead nothing more than a red herring.

Crucially, the "Notice to Users" does not apply to the action that resulted in this disclosure—namely, connecting to the internet on a computer on which CrashPlan was installed, which does not trigger the display of that notice. While Hasselbring did occasionally connect to the VPN for legitimate reasons unrelated to this lawsuit, he did not send or receive messages from, or even access, his Gmail account while so connected. [Hasselbring Decl. at ¶¶ 19, 21.] Vanderbilt certainly does not claim to have obtained any of the emails at issue as a result of Hasselbring's VPN access. Instead, Vanderbilt has repeatedly admitted that the documents at issue were obtained via CrashPlan, and that CrashPlan requires merely an internet connection, not a connection to Vanderbilt's VPN.

Vanderbilt appears to be relying on the "Notice to Users" as a kind of general statement regarding the expectations of privacy in the use of any Vanderbilt "system"—a term used but undefined in the "Notice to Users." A plain reading of the Notice, however, proves this is not the case. This Notice applies only to uses *of the Vanderbilt VPN*, not to the use of any Vanderbilt-related device generally.

This is certainly how Hasselbring understood it, [Hasselbring Decl. at ¶¶ 20, 22] and his understanding is perfectly reasonable (indeed, correct) given the language of the notice itself.

For example, in the sentence immediately preceding the much-ballyhooed warning that "USERS (AUTHORIZED OR UNAUTHORIZED) HAVE NO EXPLICT OR IMPLICIT EXPECTATION OF PRIVACY," the Notice states: "*This Enterprise SSL VPN Secure Access Service* is for authorized use only." Read in conjunction, it is apparent that this warning refers only to "users" of the VPN service.

Further, immediately following this warning, the Notice explains that "[a]ny and all uses *of the Vanderbilt Enterprise SSL VPN service* and all data *on this system* may be intercepted, [etc.]." The emphasis, again, is on the use of this particular system (the Vanderbilt VPN) specifically, not the use of any Vanderbilt system or Vanderbilt-related device generally.

Again, Vanderbilt does not contend, and Hasselbring has no reason to believe, that his use of the Vanderbilt VPN service played any role in the disclosure of the privileged emails at issue. As such, except insofar as it may show constructive notice of the Acceptable Use (for what little that's worth), the "Notice to Users" on which Vanderbilt so heavily relies is irrelevant to this Motion.

CHOICE OF LAW

Vanderbilt claims federal law applies to the question of waiver because there is federal question jurisdiction, citing *Hancock v. Dotson*, 958 F.2d 1367 (6th Cir. 1992). This law is not controlling. While *Hancock* does stand for the proposition that "the federal common law of privileges should govern all claims of privilege raised" "in federal question cases where pendent state claims are raised," other portions of the opinion clarify that this holding should apply only in "'what is primarily a federal question case.'" *Id.* at 1373 (quoting *Perringnon v. Bergen Brunswig Corp.*, 77 F.R.D. 455 (N.D. Cal. 1978)). Moreover, *Hancock* is silent on the issue presented here—namely, a privilege dispute involving a non-diverse party who is not personally facing any federal claims and has been added exclusively by virtue of the court's supplemental jurisdiction.

With respect to Hasselbring—the only Defendant involved in the instant Motion—this certainly is not "primarily a federal question case." Instead, both Vanderbilt's claims and Hasselbring's counterclaim sound exclusively in Tennessee law. Because state law governs the entirety of the dispute between Hasselbring and Vanderbilt, the *Erie* doctrine mandates that state

law govern the issue of privilege as well. *See Soehnlen v. Aultman Hospital*, 2007 WL 1342508, at *3 (N.D. Ohio May 4, 2007) ("A federal court exercising supplemental jurisdiction over state law claims [under 28 U.S.C. § 1367] is bound to apply the law of the forum state to the same extent as if it were exercising its diversity jurisdiction") (citation in original, quotation omitted); *cf. Garza v. Scott & White Mem. Hosp.*, 234 F.R.D. 617, 625 (W.D. Tex. 2005) (holding that "applying state privilege law to evidentiary materials that are related to pendent state claims, so long as they are unrelated to any federal claims" is "more faithful to the text of" Rule 501).

That said, it does not appear that Tennessee law has explicitly addressed the issue of waiver on these facts. The application of Tennessee law, therefore, will not necessarily change the analysis of the main issue in Vanderbilt's brief. It does mean, however, that the accountant-client privilege *does* apply. Tenn. Code Ann. § 62-1-116. Because Hasselbring reasonably expected those communications to remain private for the reasons discussed with respect to attorney-client communications below, the accountant privilege is also enforceable and also has not been waived. *See* Hasselbring Decl. at ¶ 6 ("I have also used my Gmail account for confidential communications with my accountant since its creation.").[5]

ARGUMENT

I. Vanderbilt agreed that there would be no waiver of the attorney-client privilege in this case [Dkt. 105].

Vanderbilt, operating on the assumption that Rule 502(b) governs, devotes the final portion of its brief to the argument that these documents were not "inadvertently disclosed" within the meaning of that Rule. Contrary to Vanderbilt's argument, Rule 502(b) is not controlling here

[5] Because Vanderbilt has refused to allow discovery before this issue was briefed, Hasselbring is unsure whether any of the emails Vanderbilt admits would otherwise be subject to the accountant-client privilege were sent from Hasselbring's Vanderbilt email account. To the extent that is even relevant given the issues with Vanderbilt's policies, Hasselbring reserves his right to present further arguments on this point after discovery may be had.

because the parties consented to, and the Court entered, an Agreed Confidentiality and Protective Order [Dkt. 105]. *See* Fed. R. Evid. 502(e), (d). When an agreement is reached under Rule 502(e) or an order is entered under Rule 502(d), it trumps Rule 502(b). For example, despite Rule 502(b), an order under Rule 502(d) "may provide for return of documents without waiver irrespective of the care taken by the disclosing party . . . ." Fed. R. Evid. 502 Advisory Committee Notes; *accord Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (noting that "so-called 'claw-back' agreements . . . allow the parties to forego privilege review altogether . . . .") (cited in Fed. R. Evid. 502 Advisory Committee Notes). In this case, the Order expressly states that "[t]he Provisions of Federal Rule of Evidence 502(b) are inapplicable to the production of privileged information under this Protective Order." [Dkt. 105 at ¶ 19.] The Order instead provides, by agreement of the parties, that it shall "operate as an order concerning waiver under, and in a manner otherwise affording the maximum protection allowed by, Federal Rule of Evidence 502(c, d, and e) and analogous law and rules of any other state or court." [*Id.*] The "analogous laws and rules of any other state or court" to which Vanderbilt agreed include Tenn. R. Evid. 502, which (unlike the Federal Rule) does not require the disclosure to be "in a . . . proceeding" for it to apply, which would result in no waiver on these facts. Similarly, Paragraph 18 of the Protective Order states: "Neither the attorney-client privilege nor the work product protection is waived by disclosure connected with this litigation." and "It is ordered that the disclosure [(note the lack of a modifier on disclosure)] of privileged, work product protected or other protected information is not a waiver in the pending case." Vanderbilt agreed to this broad language, and the Court approved it. The Court should now enforce it and hold that Hasselbring's privilege has not been waived.

II. Hasselbring had an objectively reasonable belief that his communications with his counsel, which occurred on his private, password-protected Gmail account over private, non-Vanderbilt internet connections, using his private, non-Vanderbilt electronic devices, would be confidential.

Because Hasselbring did not use any Vanderbilt systems to communicate with his counsel, those communications were not subject to Vanderbilt's policies or notices and there are no grounds for waiver merely because those emails were inadvertently disclosed to Vanderbilt through automated technical processes of which Hasselbring was unaware and took no action to implement. In the alternative, even assuming Vanderbilt's Acceptable Use Policy has some relevance to this case, Hasselbring's subjective expectation of privacy in these emails was, on balance, objectively reasonable. Either way, the privilege has been maintained.

A. Hasselbring's communications with his counsel were not performed using Vanderbilt's systems and were not covered by either the Acceptable Use Policy or the "Notice to Users."

As a threshold matter, Vanderbilt cannot justify its conduct (either intercepting the privileged communications in the first place or delaying disclosure of that fact for over three months) by relying upon the language contained in any of its policies. Vanderbilt's Acceptable Use Policy warns only that Vanderbilt reserves the right (in limited, narrowly conscribed circumstances) to inspect "records created, stored, or communicated with Vanderbilt information technology." Hasselbring had absolutely no reason to believe that his privileged communications with counsel fell within this definition—they do not. These emails were sent, received, and stored on Hasselbring's private, web-based, password protected Gmail account, which he created specifically to avoid disclosure to Vanderbilt. [Hasselbring Decl. at ¶¶ 4-6.] All the evidence suggests that the emails were only sent or received on his private, personal computers or devices. [Hasselbring Decl. at ¶ 7.] The apparent fact that the combination of (1) an automatic, unintentional process by which copies of those emails were saved to the computers identified by Mr. Sidiqyar

(which computers Hasselbring no longer even viewed as Vanderbilt property); and (2) the operation of the CrashPlan program about which Hasselbring knew nothing, caused those communications to somehow become "stored" on Vanderbilt's systems does not change the fact that, with respect to these emails, Hasselbring did not "use" Vanderbilt's systems in any meaningful way.

The "Notice to Users" is even more clearly inapplicable. As set forth above, that Notice, by its express terms, applies only when someone is actively using the Vanderbilt VPN, and the means by which Vanderbilt obtained these emails had nothing to do with Hasselbring's use of the VPN.

When communicating with his counsel, Hasselbring was not using any "Vanderbilt system," however that term may be defined. He used a private, web-based, password-protected Gmail account; privately-purchased, non-Vanderbilt devices; on a private, non-Vanderbilt internet connection. [Hasselbring Decl. at ¶¶ 4-7 & 14.] Any inadvertent synching of those messages onto a computer previously owned by Vanderbilt does not constitute a "use" of Vanderbilt's systems that would warrant application of these policies or a waiver of the attorney-client privilege.

Stengart v. Loving Care Agency, Inc. provides a perfect example of this principle at work. There, the employee used her employer-issued "laptop to access a personal, password-protected email account on Yahoo's website, through which she communicated with her attorney about her situation at work," at least some of which were likely sent or received during work hours through the company's servers. 990 A.2d 650, 656 (N.J. 2010). Upon leaving the company, the employee returned her laptop. *Id.* After the employee brought suit, employer's forensic imaging expert found several email communications between the employee and her attorney on the laptop's hard-drive. *Id.*

After failing (like Vanderbilt) to "advise opposing counsel about the e-mails until months later," *id.*, the employer argued that its policy reserving "the right to review, audit, intercept, access, and disclose all matters on the company's media systems at any time, with or without notice" resulted in a waiver of the privilege for all emails located on its systems. *Id.* at 657. "In light of the language of the Policy," the Court rejected this argument and upheld the privilege, specifically noting, in relevant part:

> [T]he Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company.

Id. at 663. As a result, "[t]he Policy did not give [the employee] or a reasonable person in her position, cause to anticipate that [her employer] would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account." *Id.* at 664. All these things are equally true of Vanderbilt's Acceptable Use Policy, which is equally inapplicable.

Other cases with similar holdings abound. For example, in *Nat'l Econ. Research Assocs., Inc. v. Evans*, the court found no waiver occurred on analogous facts, stating:

> [T]he Manual did not expressly declare, or even implicitly suggest, that [employer] would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on an [employer]-issued computer. Nor did [employer] warns its employees that the content of such Internet e-mail communications is stored on the hard disk of an [employer]-issued computer and therefore capable of being read by [the employer.]

2006 WL 2440008, at *3 (Mass. Super. Ct. Aug. 3, 2006).

Similarly, in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), an employee accessed his personal email accounts, stored on third-party computer systems (including a Gmail account) while on his work computer. *Id.* at 552. As a result, his username and password were saved to the computer. *Id.* at 552. Using that saved information,

his employer logged onto his private, web-based accounts and accessed certain privileged emails. *Id.* As in this case, those emails were sent by the employee on his own home computer, although he did not deny viewing them on his work computer. *Id.* at 553.

As Vanderbilt has done here, the employer in *Pure Power Boot Camp* relied on the email policy contained in its Employee Handbook. *Id.* at 552. And, like Vanderbilt's Acceptable Use Policy, this policy only applied to emails "stored in, created on, received from, or sent through or over *the system*." *Id.* (emphasis in original). Relying on this language, the Court held that this Policy did not remove the employee's reasonable expectation of privacy in his private, web-based accounts because he did not store them on his employer's system. *Id.* at 559-561 ("That expectation of privacy was also reasonable, as nothing in [employer]'s policy suggests that it could extend beyond Plaintiffs' own systems.").

The facts here are materially indistinguishable. While Vanderbilt used CrashPlan rather than a saved password, both employers gained access to privileged communications sent on a private computer through an employee's inadvertence (although "inadvertence" is too strong a word in Hasselbring's case). And, while the employer in *Pure Power Boot Camp* obtained only a username and password giving access to emails, whereas Vanderbilt obtained actual copies of the emails themselves, neither employee intentionally stored their private emails on their employer's system. The fact that Vanderbilt's computers apparently made copies of Hasselbring's emails instead of just his password should not change the result; this automatic process occurred without Hasselbring's knowledge and could not have affected his reasonable belief of confidentiality.

Sims v. Lakeside School, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007) is also on point. In that case, the employee sent privileged web-based emails using his employer-issued laptop. *Id.* at *2. Notwithstanding the fact that the employee "was on notice that he did not possess a

reasonable expectation of privacy in the contents of his laptop," the Court held that any copies of web-based emails found on the hard-drive of the laptop were privileged as a matter of public policy. *Id.* When, as here, the emails were not even sent on an employer-issued computer, but were instead (as best we can tell) merely automatically synched to that computer after being sent using other devices, the case for respecting efforts made to protect confidentiality and preserve the privilege are even stronger.

In sum, Hasselbring neither knew nor should have known that his emails with his attorneys had been compromised. Those communications were not a "use" of any Vanderbilt system and, as such, were not subject to Vanderbilt's policies or warnings notwithstanding any inadvertent disclosure. Because Vanderbilt admits those emails would otherwise be privileged and its waiver rests solely on those policies and notices, there are no grounds for finding that any privilege has been waived.

B. Assuming arguendo that Vanderbilt's Acceptable Use Policy is relevant, it did not negate Hasselbring's objectively reasonable expectation that his communications with counsel would remain private.

As set forth above, Hasselbring's communications with counsel did not "use" Vanderbilt's systems and were not subject to Vanderbilt's policies. Even if they were, however, the privilege still would not be waived.

When an employee uses an employer's computer system, "the question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable." *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 256-60 (Bankr. S.D.N.Y. 2005). This determination "turn[s] on the very specific factual situations unique to each case." *Sprenger v. Rector & Bd. of Visitors of Va. Tech.*, 2008 WL 2465236, at *4 (W.D. Va. June 17, 2018).

"The majority view," however, "is that the employees do not waive the privilege in material on their work computer simply because the employer can monitor their communications." *United States v. Hudson*, 2013 WL 4768084, at *9 (D. Kan. Sept. 5, 2013). After all, the attorney-client privilege is "the oldest of privileges for confidential communication known to the common law." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). As articulately explained in *United States v. Hatfield*, 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009), "a general rule holding that individuals waive privilege by storing personal documents on a company computer could have significant unintended but very damaging consequences," including "impos[ing] a severe legal prejudice for nothing more than a (possible) violation of a company's internal policy." *Id.* at *10, n.15; *see also id.* at *8 (collecting cases and concluding that "most—but not all—courts have held that employees do not waive privilege simply by maintaining documents on a company computer system"). These and other policy reasons have caused courts to hold that "where the attorney-client privilege is concerned, hard cases should be resolved in favor of the privilege, not in favor of disclosure." *United States v. Mett*, 178 F.3d 1058, 1065 (9th Cir. 1999); *see also Moss v. Unum Life Ins.*, 495 F. App.'x 583, 596 (6th Cir. 2012) (same); *In re High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *7, n.63 (N.D. Cal. Feb. 28, 2013) (invoking this principle as a tie-breaker when applying the *Asia Global* factors).

Assuming *arguendo* the Court finds Vanderbilt's Acceptable Use Policy relevant here and (with the above considerations in mind) applies *Asia Global* factors, the privilege has still been maintained.

As to the **first factor**—whether the employer maintains a policy banning personal or other objectionable use—Vanderbilt's Acceptable Use Policy does not pass muster. (For the reasons explained repeatedly above, the "Notice to Users" is completely irrelevant to this analysis and will

not be addressed.) Unlike the cases cited by Vanderbilt, the Acceptable Use Policy never forbids personal use of Vanderbilt's systems.[6] *Compare* Dkt. 163-1 at Ex. 1 *with, e.g., Pinnacle Surety Servs., Inc. v. Manion Stigger, LLP*, 370 F. Supp. 3d 745, 753 (W.D. Ky. Feb. 5, 2019) (policy stated "Personal use of the internet, including the sending and receiving of personal e-mails, is prohibited while at work").

Instead, Vanderbilt's policy only expressly forbids use that violates law or one of Vanderbilt's internal policies, and implicitly acknowledges that "sensitive personal information" may be kept on Vanderbilt's systems. This is not enough to satisfy the first factor. *See, e.g., Kreuze v. VCA Animal Hospitals*, 2018 WL 1898248, at *2 (D. Md. Apr. 20, 2018) (first factor weighs in favor of privilege when policy "does not affirmatively ban personal use by its employees" and "as written directly acknowledges that personal or non-business use of the Systems will occur"); *In re High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *6 (first factor weighs in favor of privilege where "court cannot say [employer's] policy represents an all-out ban on personal use"); *Hudson*, 2013 WL 4768084, at *9 (no waiver where policy "does not prohibit personal use of the technology equipment"); *Hatfield*, 2009 WL 3806300, at *9 (first factor weighs in favor of privilege where policy only prohibits "several specific activities" but "does not expressly prohibit employees from using their company computer to conduct personal legal matters"). It bears emphasis that Hasselbring's only arguable "use" of Vanderbilt's systems—accessing a private, password protected, web-based email account—does not fall into any of these prohibited categories and therefore was not even the type of activity the Policy was designed to detect. *See, e.g., Ala. Aircraft Indus., Inc. v. Boeing Co.*, 2016 WL 7745029, at *8 (N.D. Ala. Dec. 2, 2016)

[6] Nor does it appear that Vanderbilt faculty understand this Policy as forbidding such use of Vanderbilt-issued computers. [Hasselbring Decl. at ¶ 16.]

(first factor weighs in favor of privilege when policy is "primarily concerned with rooting out improper personal use," "seems designed to protect the substantive confidentiality of communications," and "do[es] not explicitly ban the type of behavior" at issue). The first factor favors the privilege.

The **second factor**—whether the employer monitored employees' use of email—also weighs in favor of the privilege. There is no evidence that Vanderbilt has ever before searched an employee's private, non-Vanderbilt emails—let alone the back-up files created by CrashPlan. This is certainly the first instance Hasselbring is aware of [Hasselbring Decl. at ¶ 26], and Vanderbilt has refused Hasselbring's attempts to speak with knowledgeable witnesses about whether there may have been others. For Vanderbilt's sake, we are hopeful that this is the only instance in which it has engaged in the dubious practices at issue here—namely, with full knowledge that a former employee had been represented by counsel for a year-and-a-half, learning that it had been given clearly unintentional access to that employee's privileged communications with his attorneys, then keeping it quiet for three months and allowing that former employee and his attorneys to have additional, unwittingly compromised communications in the meantime.

In any case, on this record, there is no evidence of other instances of actual monitoring, which favors the privilege. *See, e.g., Kreuze*, 2018 WL 1898248, at *2 ("Plaintiff correctly points to a number of courts that have opined that the ability of an employer to monitor an employee's communication is not sufficient to waive the attorney-client privilege; instead, evidence of actual monitoring is needed."); *Hudson*, 2013 WL 4768084, at *9 (no waiver where there was no evidence "that the [employer] actually monitored the use of technology equipment"); *In re High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *7 (second factor favored privilege when

"nothing in the record before the court suggests that [employer] actually monitored its employees' emails").

On the **third factor**—whether third parties have a right of access to the computer or the emails—the fact-specific nature of this inquiry is critical. While Vanderbilt's policy undoubtedly allowed for a right of access in certain places, Hasselbring had a reasonable belief both (i) that Vanderbilt no longer had any rights to the computers identified by Mr. Sidiqyar and (ii), even if did, it would not be able to access those computers unless he connected them to Vanderbilt's Wi-Fi or expressly gave physical or remote access to Vanderbilt's IT staff (neither of which he did). *See, e.g., Curto v. Med. World Commc'ns, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (calling fact that company-issued laptop was used in home office, so any monitoring would have been preceded by notice to Plaintiff, "particularly significant" to privilege analysis). Moreover, given the precautions taken to protect the emails at issue—creating private, web-based, password-protected account, only sending or receiving emails on that account from his personal, privately purchased devices, etc.—there was no objective reason for Hasselbring to believe Vanderbilt would have access to the emails either. The third factor therefore favors the privilege as well.

The **fourth factor**—whether employer notified the employee, or the employee was aware, of the use and monitoring policies—must also be applied with these unique facts in mind. As discussed at length above, Hasselbring reasonably believed that these policies did not apply to the conduct at issue. Being reasonably unaware that the policy applied to certain conduct is the effectively the same as being unaware of a policy at all. *See Mason v. ILS Techs, LLC*, 2008 WL 731557, at *4 (W.D.N.C. Feb. 29, 2008) (lack of knowledge of policy favors privilege). Because the purpose of this test is to determine whether Hasselbring's subjective expectation of privacy

was objectively reasonable, *Asia Global*, 322 B.R. at 258, and there was no objective reason to believe that this policy applied to the conduct at issue, this factor also favors the privilege.

In sum, even assuming the Acceptable Use Policy is relevant, all four *Asia Global* factors favor a finding that the privilege has not been waived.

CONCLUSION

Hasselbring created a private, password-protected, web-based Gmail account for the express purpose of conducting his email communications with his attorneys outside of Vanderbilt's systems. To the best of his recollection, he only ever sent or received emails on that account using one of several privately purchased, non-Vanderbilt devices, using private, non-Vanderbilt internet. Apparently as a result of Hasselbring's occasional accessing of his Gmail account while using Vanderbilt-issued computers he believed to be his own, and the surreptitious use of a powerful back-up software installed by Vanderbilt, those clearly privileged messages ended up in Vanderbilt's possession. Hasselbring had an objectively reasonable expectation that his communications with counsel would be private and has not waived any privileges. Vanderbilt's Motion should be denied and it should be ordered to return and destroy all privileged documents in its possession.

Respectfully submitted,

NEAL & HARWELL, PLC

By: /s/ Thomas H. Dundon
Aubrey B. Harwell, Jr., #2559
Thomas H. Dundon, #4539
Erik C. Lybeck, #35233
1201 Demonbreun St., Suite 1000
Nashville, TN 37203-3140
Phone: (615) 244-1713
Fax: (615) 726-0573
aharwell@nealharwell.com
tdundon@nealharwell.com
elybeck@nealharwell.com

Counsel for Ted S. Hasselbring

CERTIFICATE OF SERVICE

I hereby certify that on this the 22nd day of November, 2019, the foregoing has been served upon these individuals, via the Court's CM/ECF e-mail notification system.

Paige W. Mills
Robert E. Cooper, Jr.
Mary Leigh Pirtle
Ashleigh Karnell
BASS, BERRY & SIMS PLC
150 Third Avenue South, Suite 2800
Nashville, TN 37201
(615) 742-6200
pmills@bassberry.com
rcooper@bassberry.com
mpirtle@bassberry.com

Attorneys for Plaintiff Vanderbilt University

Michael G. Abelow
SHERRARD ROE VOIGHT & HARBISON, PLC
150 Third Avenue South, Suite 1100
Nashville, TN 37201
(615) 742-4532
mabelow@srvhlaw.com

Attorney for Defendant Houghton Mifflin Harcourt Publishing Company

Caren Decter *(pro hac vice)*
Edward H. Rosenthal *(pro hac vice)*
Matt Woleske *(pro hac vice)*
FRANKFURT, KURNIT, KLEIN & SELZ, P.C.
488 Madison Avenue
New York, NY 10022
(212) 826-5524
cdecter@fkks.com
erosenthal@fkks.com
mwoleske@fkks.com

Attorneys for Defendant Scholastic, Inc.

David J. Lender *(pro hac vice)*
Jessica Falk *(pro hac vice)*
Benjamin E. Marks *(pro hac vice)*
WEIL, GOTSHAL & MANGES
767 Fifth Avenue
New York, NY 10053
(212) 310-8000
david.lender@weil.com
jessica.falk@weil.com
benjamin.marks@weil.com

Attorneys for Defendant Houghton Mifflin Harcourt Publishing Company

Thor Y. Urness
BRADLEY ARANT BOULT CUMMINGS
1600 Division Street, Suite 700
Nashville, TN 37203
(615) 252-2384
turness@bradley.com

Attorney for Scholastic, Inc.

/s/ Thomas H. Dundon